UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/796,949	03/10/2004	John L. Cook III	71239	4498

23872 7590 09/13/2007
MCGLEW & TUTTLE, PC
P.O. BOX 9227
SCARBOROUGH STATION
SCARBOROUGH, NY 10510-9227

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	**PAPER NUMBER**
2136	
MAIL DATE	**DELIVERY MODE**
09/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/796,949	**Applicant(s)** COOK ET AL.	
	Examiner Brandon S. Hoffman	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 March 2004*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 March 2004* is/are: a)□ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☒ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-19 are pending in this office action.

Oath/Declaration

2. The oath or declaration is defective. A new oath or declaration in compliance with 37 CFR 1.67(a) identifying this application by application number and filing date is required. See MPEP §§ 602.01 and 602.02.

The oath or declaration is defective because:
It was not executed in accordance with either 37 CFR 1.66 or 1.68. Specifically, the third inventor (Henry L. Steinberg) did not fill in the date of the signature.

Drawings

3. The drawings are objected to because figures 1-6 do not contain a legend. From the figures alone, one skilled in the art would not be able to determine what is being depicted. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Objections

4. Claims 2-13 and 15-19 are objected to because of the following informalities: the preamble of claims 2-13 state “a method in accordance with claim 1.” The claims are dependent and therefore should read “the method of claim 1.” Similarly, the preamble of claims 15-19 state “a system in accordance with claim 14.” The claims are

dependent and therefore should read "the system of claim 14." Appropriate correction is required.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-12 and 14-19 are rejected under 35 U.S.C. 102(b) as being anticipated by Tuomenoksa (U.S. Patent Pub. No. 2002/0099937).

Regarding claim 1, Tuomenoksa teaches a method for securely communicating between a private computer satellite network and a public network, the method comprising the steps of:

- Providing a network firewall in the satellite network between the satellite network and the public network (fig. 6A, ref. num 617);
- Providing a secure access appliance in said satellite network (fig. 6A, ref. num 612 and 614);
- Sending an outgoing message from the secure access appliance through said firewall to the public network; creating an answer message to said outgoing message outside of said satellite network, said answer message asking the secure access appliance to open a tunnel through said firewall; sending said

answer message from the public network through said firewall into the satellite network in answer to the outgoing message; receiving said answer message at the secure access appliance (paragraph 0186, the tunnel interface module exchanges information with the first gateway);

- The secure access appliance opening a tunnel in said firewall after receiving said answer message (paragraph 0221).

Regarding claim 2, Tuomenoksa teaches further comprising:

- Providing a permitted and a forbidden network entity in the satellite network (paragraph 0159 and 0236);
- Blocking the secure access appliance from communicating with the forbidden entity (paragraph 0236, network traffic can be blocked based on the rules);
- Passing communications between the secure access appliance and the permitted network entity (paragraph 0236, network traffic can be allowed based on the rules).

Regarding claim 3, Tuomenoksa teaches wherein said blocking is performed inside the secure access appliance (fig. 6A, ref. num 617).

Regarding claim 4, Tuomenoksa teaches wherein said blocking is performed inside the secure access appliance by one of an internal network switch and a network filter (fig. 6A, ref. num 680).

Regarding claim 5, Tuomenoksa teaches wherein:

- The firewall is configured to allow outgoing type messages to pass through the firewall to the public network (paragraph 0237);
- The firewall is configured to allow answer type messages to the outgoing type messages to pass through the firewall into the satellite network (paragraph 0237).

Regarding claim 6, Tuomenoksa teaches wherein:

- The firewall is configured to allow outgoing HTTP type messages to pass through the firewall to the public network (paragraph 0238);
- The firewall is configured to allow answering HTTP type messages to the outgoing HTTP type messages to pass through the firewall into the satellite network (paragraph 0238).

Regarding claim 7, Tuomenoksa teaches wherein said firewall passes HTTP protocol messages for World Wide Web access by entities of the satellite network (paragraph 0238).

Regarding claim 8, Tuomenoksa teaches further comprising:

- Providing rules for operation of the tunnel in the secure access appliance (paragraph 0237);

- Operating the tunnel according to the rules during and after said opening of the tunnel (paragraph 0237).

Regarding claim 9, Tuomenoksa teaches wherein:

- The satellite network includes a plurality of network entities (fig. 6A, ref. num 611-616);
- The rules limit which of the network entities the tunnel can access (paragraph 0237).

Regarding claim 10, Tuomenoksa teaches wherein the rules include instructions for forming a virtual private network and a network filter (paragraph 0139).

Regarding claim 11, Tuomenoksa teaches wherein the outgoing message is a status message and is sent periodically from the satellite network through the firewall to the public network (paragraph 0163).

Regarding claim 12, Tuomenoksa teaches further comprising:

- Providing a private computer director network connected to the public network, the director network including a controller and a server (fig. 6A, ref. num 650 and 653);
- Sending the outgoing message from the satellite network to the director network; the controller sending the answer message to the satellite network asking to

open a tunnel through the firewall; the controller sending a tunnel request message to the server asking to open the tunnel with the satellite network; the server and the secure access appliance cooperating to open and operate the tunnel (paragraph 0173, the daemon is responsible for receiving the messages and sending answers);

- Providing server rules for operation of the tunnel in the server (paragraph 0236);
- Operating the tunnel at the server according to the server rules during and after the opening of the tunnel (paragraph 0237).

Regarding claim 14, Tuomenoksa teaches a system for securely communicating between a private computer satellite network and a private computer director network through a public network, the satellite network including a firewall, the system comprising:

- A secure access appliance in the satellite network sending an outgoing message through the firewall and the public network to the director network (fig. 6A, ref. num 612 and 614),
- The firewall accepting answer messages from the public network answering said outgoing message (paragraph 0186, the tunnel interface module exchanges information with the first gateway),
- Said secure access appliance including a tunnel client opening a tunnel in the firewall in response to an answer message asking said secure access appliance to open a tunnel through said firewall (paragraph 0221).

Regarding claim 15, Tuomenoksa teaches wherein said secure access appliance includes satellite rules for operation of said tunnel in the satellite network (paragraph 0237).

Regarding claim 16, Tuomenoksa teaches further comprising a plurality of network entities in the satellite network, said secure access appliance includes satellite rules for limiting which of said network entities said secure access appliance can access (fig. 6A, ref. num 611-616 and paragraph 0237).

Regarding claim 17, Tuomenoksa teaches wherein said secure access appliance includes a virtual private network device and a network filter configured according to said satellite rules (paragraph 0139).

Regarding claim 18, Tuomenoksa teaches wherein said outgoing message is a status message sent periodically from the satellite network through said firewall to the public network (paragraph 0163).

Regarding claim 19, Tuomenoksa teaches wherein:

- The director network includes a controller and a server (fig. 6A, ref. num 650 and 653),
- Said controller sending said answer message to said secure access appliance in the satellite network asking to open a tunnel through the firewall, said controller

sending a tunnel request message to said server asking to open said tunnel with the satellite network (paragraph 0173, the daemon is responsible for receiving the messages and sending answers),

- Said server includes director rules for operation of said tunnel in said server (paragraph 0236),
- Said server and said tunnel client cooperating to open and operate said tunnel according to said server and client rules (paragraph 0237).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tuomenoksa (U.S. Patent Pub. No. 2002/0099937) in view of Markham et al. (U.S. Patent No. 2004/0083382).

Regarding claim 13, Tuomenoksa teaches further comprising:

- Monitoring a parameter within the satellite network (paragraph 0147);
- Operating said secure access appliance to open said tunnel when said parameter is in a predetermined state, said monitoring including monitoring a plurality of parameters of the satellite network (fig. 36);

- Providing a network filter between the satellite network and said public network (fig. 6A, ref. num 617);
- Providing network filter rules for configuring said network filter when said parameter is in said predetermined state (paragraph 0237);
- Configuring said network filter when said policy controls said secure access appliance to open said tunnel (paragraph 0237);
- Configuring said network filter according to said network filter rules when said parameter is in said predetermined state (paragraph 0139);
- Providing packet router rules for configuring a packet router when said policy controls said secure access appliance to open said tunnel (paragraph 0232);
- Configuring said packet router according to said packet router rules when said policy controls said secure access appliance to open said tunnel (paragraph 0232);
- Said parameter is a status of the satellite network, and said predetermined state is said status being outside of predetermined acceptable limits (fig. 36);
- Said secure access appliance and a VPN server connect to form a virtual private network (paragraph 0139);
- A distributed state machine is used to control a life cycle of said virtual private network, an expert system configures said distributed state machine according to said policies, said polices are expressed as Extensible Markup Language (XML) (paragraph 0127);
- Auditing information is expressed as XML (paragraph 0127);

- Probes are defined to measure a network state or statistic on the satellite network (fig. 36, ref. num 3620, 3625, 3630);
- A plurality of probe data is aggregated and reported to a directed circuit policy manager (fig. 38);
- Said aggregation of said probe data is expressed as XML (paragraph 0127).

Tuomenoksa does not teach said operating of said secure access appliance includes providing a policy in the satellite network using said plurality of parameters to control when said secure access appliance establishes said tunnel, said policy including a state machine controlling said secure access appliance, said plurality of parameters operate said state machine; configuration of said distributed state machine is monitored for auditing purposes.

Markham et al. teaches said operating of said secure access appliance includes providing a policy in the satellite network using said plurality of parameters to control when said secure access appliance establishes said tunnel, said policy including a state machine controlling said secure access appliance, said plurality of parameters operate said state machine (paragraph 0069); configuration of said distributed state machine is monitored for auditing purposes (page 5 and 6, table 1, auditing is applied).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine policy information to control the secure access appliance in establishing a tunnel, as taught by Markham et al., with the method of Tuomenoksa. It would have been obvious for such modifications because policies allow determining if communication is authorized (see paragraph 0069 of Markham et al.).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Brandon Hoffman/
BH